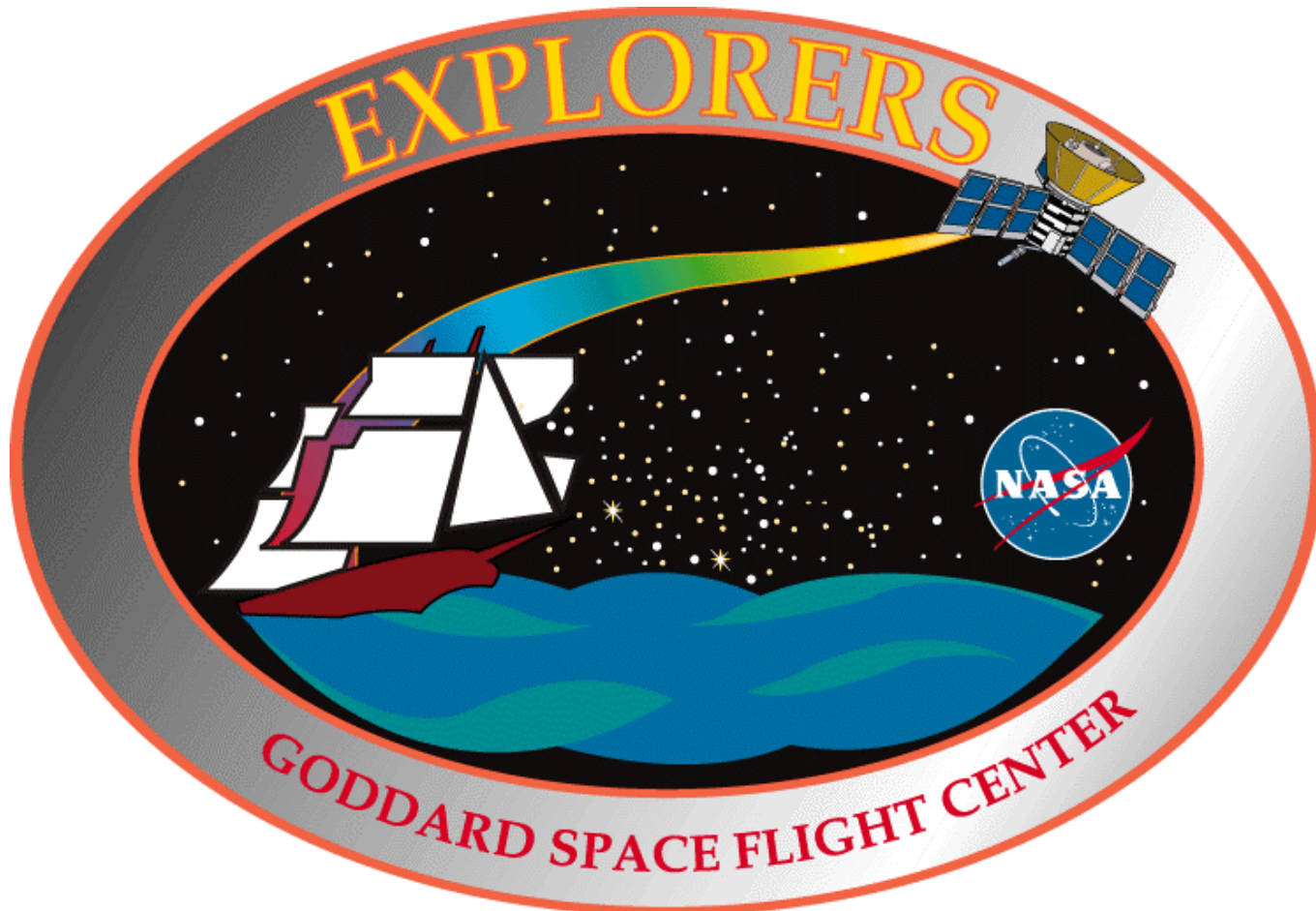


MIDEX Pre-Phase A Meetings

Safety, Reliability, & Quality Assurance Handout

Rick Claffy, GSFC Code 410/303, X6-7866



April, 2002 Teleconferences

MIDEX Pre-Phase A Meetings Handout

- **SR&QA effort is controlled by MIDEX AO, EPL Reference Document #32, containing both Requirements & Guidelines.**
 - Page 7, Par. 2.1 discusses EXP Program Office & PI joint effort to define best mix of roles and responsibilities for SR&QA execution.
 - Mission Definition & Requirements Agreement. (EPL Ref. #39)
 - Code 410/PI SR&QA Insight Agreement.
 - Signed by Phase C/D Contract, and a condition for mission confirmation.
 - Defines Early the Inter-Institutional Partnering & Funding for SR&QA services.
 - Par. 2.1 requires PIs to implement a product assurance program consistent with ISO 9000 series ANSI/ASQC Q9001-1994, covering flight hardware, software & GSE.
 - ISO registration not required, but “compliance” is expected with the Standard’s sections where it makes good engineering and programmatic sense, & as necessary to meet Explorers ISO needs for PI Missions.
 - PI SR&QA Program must meet MIDEX Safety, Reliability, and Quality Assurance Requirements, as published in AO Document #32.
 - PI Institution Quality Manual is deliverable for Explorers Program Office Review/Comment during Phase B.
 - Tailoring allowed in most assurance technology areas, but ...
 - The highly specialized discipline of System Safety, including the Range Safety effort, is dictated external to GSFC. Expert guidance through the process has always been needed by PI teams.

MIDEX Pre-Phase A Meetings Handout

- **The MIDEX SR&QA Requirements document also addresses Missions of Opportunity, LDB Missions, NSTS Payloads.**
 - **Permits further tailoring for reduced scope of MOs.**
 - **Shuttle proposers should refer to EPL Doc #34 for System Safety scope & resulting cost planning.**
 - **LDB Proposers to use Balloon Appendix to Document #32.**
- **MIDEX SR&QA document Highlights:**
 - **Requires Monthly Assurance Status Reports.**
 - **Requires supplier audits.**
 - **Requires a PI Failure Reporting System for Phase C/D/E.**
 - **Invokes Hi-Reliability Workmanship standards.**
 - **Requires flight Printed Wiring Board Coupon DPA by certified facility prior to population with flight EEE parts.**

MIDEX Pre-Phase A Meetings Handout

- **Lays out Design Review Requirements.**
 - Peer Review emphasis, with closed loop tracking of RFAs.
 - System level Review process now integrated with NASA independent Red Team functions via GSFC Quality Management System (QMS).
- **Details specific System Safety program requirements and deliverables with process flow descriptions (EPL Docs. #33-36).**
 - Magnitude of System Safety effort must not be under-estimated.
 - Allocate/identify roles & resources.
 - Start early.
 - GSFC can help in numerous ways.
- **Minimum EEE Parts criteria per GSFC 311-INST-001, Rev- for Grade 3.**
 - PI shall maintain and review Parts Lists with GSFC.
 - PI shall use an organized system to manage parts application, evaluation, and traceability.
 - GSFC PMC requires all GSFC managed missions to provide GIDEP Alert, NASA Advisory, and GSFC inter-project parts issue responses.

MIDEX Pre-Phase A Meetings Handout

- Standard Materials and Processes program required, including Contamination Controls.**
- Reliability**
 - Risk assessments made and mitigation strategies identified.**
 - FMEAs at subsystem/box level.**
- Software**
 - Code to be structured, error free, and maintainable.**
 - Establish & document SW requirements, external interface specs, user guides.**
 - Internal (peer) and external software design reviews.**
 - Use of SW Quality Metrics & Complexity analyses to augment IV&V.**
- Verification**
 - Verification/test program to ensure all mission requirements are met.**
 - Documentation to include verification matrix, environments matrix, and test procedures.**

MIDEX Pre-Phase A Meetings Handout

- **NIAT Requirements to be placed in CDRLs:**
 - **Red Team Component of Integrated System Level Reviews.**
 - Reviewer expectations can exceed baseline review requirements.
 - Extended scope, detailed questions.
 - RFA trail & Failure Report closures thoroughly checked by Red Team.
 - NASA Policy is that Code 301 Chairs all System Level Reviews for PI Missions.
 - **Significant Emphasis On Reliability Analysis:**
 - Probabilistic Risk Assessment (PRA) Recommend Start in Ph A.
 - Fault Tree Analysis, Event Sequence Diagrams, etc.
 - FMEA @ subsystem level.
 - Identify all single string design features.
 - Failure Impacts/mitigation.
 - **Tangible Continuous Risk Tracking & Management System.**
 - **PI Software QA effort and IV&V.**
 - Each mission evaluated for SW Complexity/Reliability/Risk.
 - Determination of appropriate level of NASA IV&V Facility involvement via standardized criteria.
- **Mission Success is GSFC Center Director's Ultimate Responsibility to NASA Administrator.**